



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/818,699	03/27/2001	Doug L. Rollins	MPATENT.163A	9926

20995 7590 04/17/2007  
KNOBBE MARTENS OLSON & BEAR LLP  
2040 MAIN STREET  
FOURTEENTH FLOOR  
IRVINE, CA 92614

EXAMINER
----------

NGUYEN, MINH DIEU T

ART UNIT	PAPER NUMBER
----------	--------------

2137

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	04/17/2007	ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 04/17/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

jcarter@kmob.com  
eOAPilot@kmob.com

# Office Action Summary

Application No.

09/818,699

Applicant(s)

ROLLINS, DOUG L.

Examiner

Minh Dieu Nguyen

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 30 January 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1,5,7,8,11-14,16,17,19 and 20 is/are pending in the application.
- 4a) Of the above claim(s) 2-4,6,9,10,15 and 18 is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,5,7,8,11-14,16,17,19 and 20 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 January 2007 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

## **DETAILED ACTION**

### ***Response to Amendment***

1. This action is in response to the communication dated 1/30/07 with the amendments to claims 1, 5 and 8 and the cancellation of claims 2-4, 6, 9-10, 15 and 18.
2. Claims 1, 5, 7-8, 11-14, 16-17 and 19-20 are pending.

### ***Response to Arguments***

3. Applicant's arguments filed 1/30/07 have been fully considered but they are not persuasive. The applicant argues that the combination of Simmons and Brundett does not teach checking in the client computer system an attribute of the requested data to determine whether the requested data is encrypted with an encryption key, wherein the attribute is alterable by a network administrator, and wherein the network administrator is independent of the at least one network server. The examiner respectfully disagrees, Brundett discloses checking an attribute to determine whether the requested data is encrypted with an encryption key (see Brundett: col. 13, lines 20-21; Fig. 12, element 1204), wherein the attribute is alterable by a network administrator (i.e. an administrator sets up a domain policy for EFS to become operational, see Brundett: col. 19, lines 2-4), besides, as well-known in the networking world, a network administrator could create and change attributes of the file system) and wherein the network administrator is independent of the at least one network server (i.e. the EFS architecture is implemented

in both stand-alone as well as in the network environment, see Brundett: col. 18, line 66 to col. 19, line 4).

The applicant argues that neither Simmons, nor Brundett store encrypted files and send encrypted files to the requestor. The examiner respectfully disagrees, Simmons discloses sending encrypted data files to the requestor (see Abstract, as admitted by the applicant) and Brundett discloses storing encrypted data files (see Abstract, as admitted by the applicant).

***Claim Rejections - 35 USC § 112***

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 1, 5 and 8 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The amended limitations "(checking) in the client computer system" and "wherein the network administrator is independent of the at least one network server" are not properly described in the application as filed (specification, page 12, lines 14-15 and page 13, lines 9-17, correspondingly). On page 12, lines 14-15, it is disclosed that "At block 102, the network server checks the status of an encryption attribute associated with the file", there is no information regarding

Art Unit: 2137

"checking in the client computer system", and further, the client sends a request for a file to a network server in the previous step (block 100), the requested data and its attribute are with the network server, therefore it is not proper to check in the client computer system an attribute of the requested data (to determine whether the requested data is encrypted with an encryption key).

### ***Specification***

6. The amendment filed 1/30/07 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: (checking) in the client computer system and wherein the network administrator is independent of the at least one network server.

Applicant is required to cancel the new matter in the reply to this Office Action.

### ***Claim Rejections - 35 USC § 103***

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2137

8. Claims 1, 8, 11-12 and 16-17 and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Simmons et al. (2001/0039659) in view of Brundett et al. (6,249,866).

a) As to claims 1 and 8, as best understood, Simmons discloses a method for transferring data over a computer network from a network server to a client computer system (see Simmons: 0001), the method comprising: receiving a request by a requestor using a client computer system for data from at least one network server (see Simmons: 0006); if the requested data is unencrypted (see Brundett), automatically retrieving the encryption key associated with the requestor from the client computer system; encrypting the requested data with the encryption key associated with the requestor automatically and without user intervention to create encrypted data and sending the encrypted data to the client computer system (see Simmons: 0016, 0041, 0046). Simmons is silent on the capability of checking in the client an attribute to determine whether the requested data is encrypted with an encryption key; wherein the attribute is alterable by a network administrator, and wherein the network administrator is independent of the at least one network server; if the requested data is encrypted with the encryption key. Brundett is relied on for the teaching of checking an attribute to determine whether the requested data is encrypted with an encryption key (see Brundett: col. 13, lines 20-21; Fig. 12, element 1204), wherein the attribute is alterable by a network administrator (i.e. an administrator sets up a domain policy for EFS to become operational, see Brundett: col. 19, lines 2-4), besides, as well-known in the networking world, a network administrator could create and change attributes of the file

Art Unit: 2137

system) and wherein the network administrator is independent of the at least one network server (i.e. the EFS architecture is implemented in both stand-alone as well as in the network environment, see Brundett: col. 18, line 66 to col. 19, line 4); if the requested data is encrypted with the encryption key (see Brundett: Fig. 12, element 1204), sending the encrypted data to the client computer system (see Simmons: 0046). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of checking an attribute to determine whether the requested data is encrypted with an encryption key; if the requested data is encrypted with the encryption key, wherein the attribute is alterable by a network administrator, and wherein the network administrator is independent of the at least one network server and if the requested data is encrypted with the encryption key in the system of Simmons, as Brundett teaches, so as to provide security of those files that are determined to be protected.

b) As to claims 11, 16 and 19, examiner takes official notice that sending notification, warning and alert messages are well-known in the network communication and what is in the message purely a design choice.

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of sending a notification message to inform users with more information.

c) As to claims 12, 17 and 20, please see addressed claim 1.

Art Unit: 2137

9. Claim 5, as best understood, is rejected under 35 U.S.C. 103(a) as being unpatentable over Simmons et al. (2001/0039659) in view of Brundett et al. (6,249,866) and further in view of Schneier (Applied cryptography).

The majority of this claim is in claim 1 with the addition of the following limitation: automatically generating independently of information from a network server a public encryption key and a corresponding private encryption key in a client computer system; storing the public encryption key and the corresponding private encryption key in the client computer system (see Simmons: 0041). Simmons is silent on the capability of associating an attribute with a data file, the attribute indicating whether the data file is encrypted with the public encryption key when stored on the network server, and the attribute indicating an owner of the public encryption key. Brundett discloses associating an attribute with a data file, the attribute indicating whether the data file is encrypted with the public encryption key when stored on the network server, and the attribute indicating an owner of the public encryption key (see Brundett: Fig. 7, file metadata; col. 13, lines 20-21; col. 8, lines 30-45; col. 14, lines 56-66). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of associating an attribute with a data file, the attribute indicating whether the data file is encrypted with the public encryption key when stored on the network server, and the attribute indicating an owner of the public encryption key in the system of Simmons, as Brundett teaches so as to provide security of those files that are determined to be protected. Simmons and Brundett disclose encryption keys however they do not specifically disclose public and private encryption key where the data file is encrypted



with public key. Schneier discloses public key algorithm where often the encryption key is called the public key and the decryption key is called private key (pages 4-5). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of public key algorithm in the system of Simmons and Brundett, as Schneier, teaches so as to efficiently encrypt data files.

10. Claims 7 and 13-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Simmons et al. (2001/0039659) in view of Brundett et al. (6,249,866) in view of Schneier (Applied cryptography) and further in view of Eldridge et al. (6,094,721).

Simmons, Brundette and Schneier do not explicitly disclose the public and private keys are based on a password.

Eldridge discloses a method and apparatus for updating the password status of one of more servers in a client/server environment comprising public and corresponding private key derived from password (col. 5, lines 33-46).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of generating public and private key from a password as Eldridge teaches in the system of Simmons, Pardikar and Schneier so as to secure password access.

### ***Conclusion***

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

Art Unit: 2137

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
mdh  
4/11/07

  
EMMANUEL MOISE  
SUPERVISORY PATENT EXAMINER